



USPTO

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

+"key setting"

SEARCH

THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Published before October 2002

Terms used **key setting**

Found 11 of 134,482

Sort results by

relevance

[Save results to a Binder](#)Try an [Advanced Search](#)

Display results

expanded form

[Search Tips](#)Try this search in [The ACM Guide](#)
☐ Open results in a new window

Results 1 - 11 of 11

Relevance scale ☐ ☐ ☐ ☐ ☐
 1 [Complete characterization of security notions for probabilistic private-key encryption](#)


Jonathan Katz, Moti Yung

 May 2000 **Proceedings of the thirty-second annual ACM symposium on Theory of computing**

Publisher: ACM Press

 Full text available: pdf(973.62 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

 2 [Incremental cryptography and application to virus protection](#)


Mihir Bellare, Oded Goldreich, Shafi Goldwasser

 May 1995 **Proceedings of the twenty-seventh annual ACM symposium on Theory of computing**

Publisher: ACM Press

 Full text available: pdf(1.65 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

 3 [Public-key cryptosystems provably secure against chosen ciphertext attacks](#)


M. Naor, M. Yung

 April 1990 **Proceedings of the twenty-second annual ACM symposium on Theory of computing**

Publisher: ACM Press

 Full text available: pdf(1.10 MB) Additional Information: [full citation](#), [citations](#), [index terms](#)

 4 [A short discussion of interprocess communication in the sue/360/370 operating system](#)


Richard C. Holt, Marc S. Grushcow

 January 1973 **ACM SIGPLAN Notices , Proceeding of ACM SIGPLAN - SIGOPS interface meeting on Programming languages - operating systems**, Volume 8 Issue 9

Publisher: ACM Press

 Full text available: pdf(400.93 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This paper presents the interprocess communication/synchronization scheme used in the SUE operating system. This scheme is based on a tree structure of processes which are called "facilities" and three primitive operations: Facility Call, Accept Facility Call, and Complete Facility Call. These primitives are implemented by a small "Kernel" which is the basis of the operating system.

5 Extensible file system (ELFS): an object-oriented approach to high performance file I/O



John F. Karpovich, Andrew S. Grimshaw, James C. French

October 1994 **ACM SIGPLAN Notices , Proceedings of the ninth annual conference on Object-oriented programming systems, language, and applications OOPSLA '94**, Volume 29 Issue 10

Publisher: ACM Press

Full text available: pdf(1.84 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Scientific applications often manipulate very large sets of persistent data. Over the past decade, advances in disk storage device performance have consistently been outpaced by advances in the performance of the rest of the computer system. As a result, many scientific applications have become I/O-bound, i.e. their run-times are dominated by the time spent performing I/O operations. Consequently, the performance of I/O operations has become critical for high performance in these applicatio ...

6 Simple authenticated key agreement protocol resistant to password guessing attacks



Her-Tyan Yeh, Hung-Min Sun

October 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue 4

Publisher: ACM Press

Full text available: pdf(482.32 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

Password-based mechanism is the widely used method for user authentication. Many password-based authenticated key exchange protocols have been proposed to resist password guessing attacks. In this paper, we present a simple authenticated key agreement protocol called SAKA which is simple and cost-effective. To examine its security, we provide a formal proof of security to show its strength against both passive and active adversaries. Compared with the previously best protocols, SAKA

Keywords: cryptography, key agreement, key exchange, password authentication, provable security

7 ID-based secret-key cryptography



Marc Joye, Sung-Ming Yen

October 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 4

Publisher: ACM Press

Full text available: pdf(513.15 KB)

Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)

This paper introduces *ID-based secret-key cryptography*, in which secret keys are privately and uniquely binded to an identity. This enables to extend public-key cryptography features at the high throughput rate of secret-key cryptography. As applications, efficient login protocols, an enhanced version of Kerberos, and an ID-based MAC algorithm are presented. ID-based systems were initially developed in the context of public-key cryptography by removing the need of explicit public keys. The ...

Keywords: ID-based systems, Kerberos, MACs, authentication protocols, one-time passwords, secret-key cryptography

8 A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract)



Mihir Bellare, Ran Canetti, Hugo Krawczyk

May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing**

Publisher: ACM Press

Full text available: pdf(1.61 MB)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

9 Provably secure session key distribution: the three party case

Mihir Bellare, Phillip Rogaway

May 1995 **Proceedings of the twenty-seventh annual ACM symposium on Theory of computing**

Publisher: ACM Press

Full text available: pdf(1.28 MB)

Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)10 Towards practical "proven secure" authenticated key distribution

Yvo Desmedt, Mike Burmester

December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(382.53 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Secure key distribution is a critical component in secure communications. Finding 'proven secure' practical key distribution systems is one of the major goals in cryptography. The Diffie-Hellman variants, a family of key distribution systems, achieve some of the objectives of this goal. In particular, the 'non-paradoxical' system (by Matsumoto-Takashima-Imai and Yacobi) is claimed to be secure against a known-key attack. In this paper we show that the argument used to prove this is ...

11 Monitoring user actions in the hypertext system "HyperMan"

A. Myka, U. G ntzler, F. Sarre

November 1992 **Proceedings of the 10th annual international conference on Systems documentation**

Publisher: ACM Press

Full text available: pdf(1.11 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The hypertext system "HyperMan" provides for an automatic conversion of linear machine-readable documents into hypertexts by applying text partitioning and link generation methods. After completion of the generation process, the graphical user interface of the system enables users to browse through the converted documents very easily. To determine whether user actions allow conclusions to be drawn about a generated hypertext, a special component that records user actions h ...

Results 1 - 11 of 11

The ACM Portal is published by the Association for Computing Machinery. Copyright   2006 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)



USPTO

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☒ The ACM Digital Library ☐ The Guide

+"setting key"

SEARCH

THE ACM DIGITAL LIBRARY


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Published before October 2002

Terms used **setting key**

Found 8 of 134,482

Sort results by

relevance

[Save results to a Binder](#)Try an [Advanced Search](#)

Display results

expanded form

[Search Tips](#)Try this search in [The ACM Guide](#)
☐ Open results in a new window

Results 1 - 8 of 8

Relevance scale ☐ ☐ ☐ ☐ ☐

1 [A preliminary step towards a language for picture control in a real-time mode](#)



Lou Katz, Bill Etra

 April 1976 **ACM SIGPLAN Notices , ACM SIGGRAPH Computer Graphics , The papers of the ACM symposium on Graphic languages**, Volume 11 , 10 Issue 6 , 1

Publisher: ACM Press

Full text available: pdf(557.25 KB)

 Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

With the proliferation of extremely complex analog systems for the control of television images it has become evident that some more efficient system has to be found for dealing with the mire of knobs, switches, levers, and patch cords which make up any video processing device. In planning an attack on this situation, we soon realized that a major aspect of the problem is a linguistic one. Television has only a few terms which deal with the almost infinite number of effects possible in any ...

2 [Main-memory index structures with fixed-size partial keys](#)



Philip Bohannon, Peter McIlroy, Rajeev Rastogi

 May 2001 **ACM SIGMOD Record , Proceedings of the 2001 ACM SIGMOD international conference on Management of data SIGMOD '01**, Volume 30 Issue 2

Publisher: ACM Press

Full text available: pdf(185.51 KB)

 Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The performance of main-memory index structures is increasingly determined by the number of CPU cache misses incurred when traversing the index. When keys are stored indirectly, as is standard in main-memory databases, the cost of key retrieval in terms of cache misses can dominate the cost of an index traversal. Yet it is inefficient in both time and space to store even moderate sized keys directly in index nodes. In this paper, we investigate the performance of tree structures suitable for ...

Keywords: B-trees, T-tree, cache coherence, key compression, main-memory indices

3 [Micro emulation: When to do it and when not to do it](#)



Lee Hoevel

 September 1973 **Conference record of the 6th annual workshop on Microprogramming**

Publisher: ACM Press

Full text available: pdf(723.79 KB)

 Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

In this paper, we will attempt to analyze those conditions under which the use of a nontrivial interpreter will enhance the performance of a two-phase processing system.

This analysis is couched in terms of a search for an "ideal" DEL, given a particular source language SL and base machine M. This "ideal" DEL would minimize the overall space and time needed to evaluate a typical SL program. There are two obvious choices f ...

4 Design and implementation of an agent-based intermediary infrastructure for electronic markets



Gaurav Tewari, Pattie Maes

October 2000 **Proceedings of the 2nd ACM conference on Electronic commerce**

Publisher: ACM Press

Full text available: pdf(447.73 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Keywords: electronic commerce, electronic markets, highly mediated communications, intermediaries, merchant brokering, negotiation, product brokering, software agents, utility theory

5 Implementations for coalesced hashing



Jeffrey Scott Vitter

December 1982 **Communications of the ACM**, Volume 25 Issue 12

Publisher: ACM Press

Full text available: pdf(1.64 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The coalesced hashing method is one of the faster searching methods known today. This paper is a practical study of coalesced hashing for use by those who intend to implement or further study the algorithm. Techniques are developed for tuning an important parameter that relates the sizes of the address region and the cellar in order to optimize the average running times of different implementations. A value for the parameter is reported that works well in most cases. Detailed graphs explain ...

Keywords: analysis of algorithms, assembly language, asymptotic analysis, average-case, coalesced hashing, coalsced hashing, data structures, databases, deletion, hashing, optimization, secondary storage

6 Toward a Theory of Enumerations



Paul R. Young

April 1969 **Journal of the ACM (JACM)**, Volume 16 Issue 2

Publisher: ACM Press

Full text available: pdf(1.07 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

An attempt is made to show that there is much work in pure recursion theory which implicitly treats computational complexity of algorithmic devices which enumerate sets. The emphasis is on obtaining results which are independent of the particular model one uses for the enumeration technique and which can be obtained easily from known results and known proofs in pure recursion theory. First, it is shown that it is usually impossible to define operators on sets by examining the str ...

7 Fibonacci heaps and their uses in improved network optimization algorithms



Michael L. Fredman, Robert Endre Tarjan

July 1987 **Journal of the ACM (JACM)**, Volume 34 Issue 3

Publisher: ACM Press

Full text available: pdf(1.52 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

In this paper we develop a new data structure for implementing heaps (priority queues). Our structure, Fibonacci heaps (abbreviated F-heaps), extends the binomial queues

proposed by Vuillemin and studied further by Brown. F-heaps support arbitrary deletion from an n -item heap in $O(\log n)$ amortized time and all other standard heap operations in $O(1)$ amortized time. Using F-heaps we are able ...

8 Information systems personnel as expatriates: a review of the literature and identification of issues



Fred Niederman

May 1992 **Proceedings of the 1992 ACM SIGCPR conference on Computer personnel research**

Publisher: ACM Press

Full text available:  pdf(978.96 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

Results 1 - 8 of 8

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)

Google

[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

"communication range restriction"

Search

[Advanced Search](#)
[Preferences](#)

Web

Results 1 - 5 of about 7 for "**communication range restriction**". (0.25 seconds)

Tip: Try removing quotes from your search to get more results.

Encryption key setting system, access point, encryption key ...

[0017] an encryption key setting module that, when the wireless communication range is restricted by said **communication range restriction** module, ...
www.freshpatents.com/Encryption-key-setting-system-access-point-encryption-key-setting-method-and-authent... - 29k - [Cached](#) - [Similar pages](#)

Encryption key setting system, access point, encryption key ...

The encryption key setting system in accordance with claim 1 or 2, wherein said **communication range restriction** module comprises: first means that performs ...
www.freshpatents.com/Encryption-key-setting-system-access-point-encryption-key-setting-method-and-authent... - 23k - Supplemental Result - [Cached](#) - [Similar pages](#)
[More results from www.freshpatents.com]

[PDF] Controlling formations of multiple mobile robots with inter-robot ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)
the limited **communication range restriction**. This framework can be extended to the multiple robot. case, where the platoon of robot can be divided into ...
www.araa.asn.au/acra/acra2005/papers/ha.pdf - [Similar pages](#)

Encryption key setting system, access point, encryption key ...

[0014] The **communication range restriction** module may have any of various ... The access point includes: a **communication range restriction** module that ...
www.patentdebate.com/PATAPP/20040076300 - Supplemental Result - [Similar pages](#)

Encryption key setting system, access point, encryption key ...

A variety of embodiments can be considered as embodiments for realizing a **communication range restriction** module. For example, it is also possible to ...
www.patentdebate.com/PATAPP/20050201557 - Supplemental Result - [Similar pages](#)

In order to show you the most relevant results, we have omitted some entries very similar to the 5 already displayed.

If you like, you can repeat the search with the omitted results included.

Free! Speed up the web. [Download the Google Web Accelerator](#).

"communication range restriction"

Search

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2006 Google

[Google](#)

[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

"restricting communication range"

[Search](#)

[Advanced Search](#)
[Preferences](#)

Web

Results 1 - 2 of 2 for "**restricting communication range**". (0.17 seconds)

Tip: Try removing quotes from your search to get more results.

[A Local Facility Location Algorithm for Sensor Networks](#)

This is because they allow **restricting communication range** of the sensor to the minimum which still provide full system connectivity, because they can ...

www.cs.rpi.edu/news/colloquia/Feb01_2005.html - 17k - [Cached](#) - [Similar pages](#)

[Communications Jamming? \[Archive\] - BeyondUnreal Forums](#)

... all team based communications fully public. Or **restricting communication range** to vocal distances (and also being able to be heard by the opposing team) ...

forums.beyondunreal.com/archive/index.php/t-101714.html - 8k - Supplemental Result - [Cached](#) - [Similar pages](#)

"restricting communication range"

[Search](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2006 Google

Google

[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

restricted communication "setting encryption k

Search

[Advanced Search](#)
[Preferences](#)**Web**Results 1 - 8 of about 21 for **restricted communication "setting encryption key"**. (0.27 seconds)

Tip: Save time by hitting the return key instead of clicking on "search"

Mandriva Club . Mandriva Linux 2006 now available for Club members!iwconfig wlan0 mode Managed-echo " --**Setting encryption key**" iwconfig wlan0 key**restricted** 7DC0E6358666EXXXXXXXX echo "Bringing up interface wlan0. ...

club.mandriva.com/xwiki/bin/view/Main/2006launch - 194k - Cached - Similar pages

[PDF] Deployment Guide Series: IBM Tivoli Monitoring 6.1

File Format: PDF/Adobe Acrobat

understanding the **communication** flow among the IBM Tivoli Monitoring 6.1 ... runGSkit :**setting encryption key**. Enter a 32-character encryption key, ...

www.redbooks.ibm.com/redbooks/pdfs/sg247188.pdf - Similar pages

[PDF] WatchGuard LiveSecurity System User Guide

File Format: PDF/Adobe Acrobat

and documentation are provided with **Restricted Rights**. ... Automatically block all**communication** from a source site ... **setting encryption key** ...

www.watchguard.com/help/docs/v45userguide.pdf - Similar pages

[PDF] NDS-AS User Guide and Reference

File Format: PDF/Adobe Acrobat

Because this file contains the encryption key used for **communications** with Agents,access to the. Client configuration file should be **restricted**. ...

www.novell.com/documentation/authserv/pdfdoc/userguide.pdf - Similar pages

[PDF] ORiNOCO AP-2000 User Guide

File Format: PDF/Adobe Acrobat

packets from the EMPLOYEE workgroup, could, in contrast, be **restricted** ... This exampledescribes **setting encryption Key 1** on the wireless card in Slot A. ...

ftp2.ua.freebsd.org/pub/radio/software/AP2K/UG-AP2000-ORiNOCO-UK.pdf - Similar pages

[PDF] ORiNOCO AP-2000 User Guide

File Format: PDF/Adobe Acrobat

certain ports on AP-2000 devices to control the path of **communication** ... This exampledescribes **setting encryption Key 1** on the wireless card in Slot A. ...

www.moonblinkwifi.com/files/AP-2000.pdf - Similar pages

[PDF] Deployment Guide Series: IBM Tivoli Monitoring V 6.1

File Format: PDF/Adobe Acrobat

Note to U.S. Government Users **Restricted Rights** -- Use, duplication or disclosure ...runGSkit : create certificate. runGSkit : **setting encryption key**. ...

www.cressida.info/pdfs/sg247188.pdf - Similar pages

[PDF] hp WL520 enterprise access point user guide

File Format: PDF/Adobe Acrobat

HP WL520 devices and select a free or relatively unused **communication** ... This exampledescribes **setting encryption Key 1** on the wireless card in Slot A. ...

www.hp.com/rnd/pdfs/hp_enterprise_ap_ugnew.pdf - Similar pages

In order to show you the most relevant results, we have omitted some entries very similar to the 8 already displayed.

If you like, you can repeat the search with the omitted results included.

Free! Get the Google Toolbar. [Download Now](#) - [About Toolbar](#)



restricted communication "setting en

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2006 Google